

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA**

UNITED STATES OF AMERICA,

Plaintiff,

vs.

CHAD A. POWERS,

Defendant.

)
)
)
)
)
)
)
)
)
)
)

8:09CR361

**FINDINGS AND
RECOMMENDATIONS**

This matter is before the court on defendant Chad A. Powers' (Powers) Motion to Dismiss for Improper Venue ([Filing No. 16](#)) and Motion to Dismiss the Indictment ([Filing No. 18](#)). Powers filed pre-hearing briefs (Filing Nos. [17](#) and [19](#)) in support of his motions. The government filed a brief ([Filing No. 23](#)) in opposition to Powers' motions. Powers is charged in the Indictment ([Filing No. 1](#)) with intentionally exceeding authorized access to a computer, and thereby obtaining information from a protected computer from March 3, 2009, through March 14, 2009, in violation of [18 U.S.C. § 1030\(a\)\(2\)\(C\)](#). The alleged offense was committed in furtherance of a tortious act in violation of the laws of the State of Nebraska, specifically, invasion of privacy and intentional infliction of emotional distress. **See** [Filing No. 1](#) - Indictment.

On January 28, 2010, the court held an evidentiary hearing on Powers' motions. Powers was present with his counsel, Federal Public Defender David R. Stickman. Assistant U.S. Attorney Frederick D. Franklin represented the United States. The court received into evidence two exhibits: an affidavit in support of a search warrant (Ex. 101) and miscellaneous discovery from the government (Ex. 102). **See** [Filing No. 28](#) - Exhibit List. Theresa Hiner (Hiner), employed by the Federal Public Defenders Office to manage computer and network systems, testified during the hearing ([Filing No. 25](#) - Witness List). A transcript (TR.) of the hearing was filed February 3, 2010 ([Filing No. 33](#)), whereupon the motion was deemed submitted.

FINDINGS OF FACT

On or about March 3, 2009, through March 14, 2009, approximately eight images of Shaunna M. Briles (Briles), partially nude and/or engaging in provocative poses, were sent via her America Online (AOL) e-mail account and addressed to individuals in her account address

book (Ex. 101, p. 3). Briles was an Omaha, Nebraska resident at the time of the incident (Ex. 102, p. 2). Additional e-mails were sent to e-mail addresses Briles did not recognize (Ex. 101, p. 3). Some e-mails were sent to recipients in Nebraska, including a coworker (TR. 38; Ex. 102, p. 1). Briles, the registered holder of the e-mail account, intentionally gave the authorization password to Powers (TR. 3). Powers used the password to gain access to the e-mail account (TR. 3). The images contained in the e-mails were taken in 2003, and Briles had previously e-mailed the images to someone on a previous occasion (Ex. 101, p. 4). With authorized access to Briles' e-mail account, Powers was able to gain access to past e-mail messages in the account, and could subsequently access the images by exceeding the purpose for which the password was given (TR. 5).

Briles contacted Federal Bureau of Investigation (FBI) Special Agent Justin Kolenbrander (Special Agent Kolenbrander) on or about March 17, 2009, regarding the computer intrusion (Ex. 101, p. 3). On or about March 18, 2009, Special Agent Kolenbrander interviewed Briles about the e-mail messages and the images (Ex. 101, p. 4). Briles told Special Agent Kolenbrander three of the e-mail messages were sent from her AOL e-mail account on March 3, 2009, March 4, 2009, and March 14, 2009 (Ex. 101, p. 4). Briles stated she became aware of the sent e-mail messages on or about March 5, 2009, after she noticed copies of three e-mail messages in her AOL e-mail account (Ex. 101, p. 4).

The same day, after the interview, Briles telephoned Special Agent Kolenbrander and stated her sister, Stacy Mueller (Mueller), received one of the e-mail messages on her work account at the Iowa Department of Public Safety (Ex. 101, p. 4). Special Agent Kolenbrander contacted Mueller's supervisor, Steven Ray (Ray), and requested copies of the e-mail message headers for March 4, 2009, and March 14, 2009 (Ex. 101, p. 4). On or about March 25, 2009, Special Agent Kolenbrander received a CD-ROM from Ray containing digital copies of the e-mail messages and the attached images (Ex. 101, p. 4-5).

Analysis of the March 4, 2009, and March 14, 2009, e-mail messages included on the CD-ROM show the e-mail messages originated from the Internet Protocol ("IP") Address 68.230.83.202 (Ex. 101, p. 5). An IP Address is a unique numeric address used to identify computers on the Internet (Ex. 101, p. 2). The IP Address obtained from the e-mail messages was registered to Cox Communications in Atlanta, Georgia (Ex. 101, p. 5). Pursuant to a subpoena, Cox Communications provided subscriber information to confirm the IP Address

68.230.83.202 belonged to Powers, 2811 W. Deer Valley Road, Apartment 1029, Phoenix, Arizona, from January 10, 2009, through March 18, 2009 (Ex. 101, p. 5). Thereafter, FBI Special Agent Michael Boady (Boady) filed an affidavit in support of a search warrant on May 29, 2009 (Ex. 101, p. 1).

At the evidentiary hearing, Hiner testified regarding use and access to computers and e-mail accounts (TR. 24). Hiner stated a person is not required to have a home computer to have an e-mail account (TR. 25). An individual can use a public computer to access an e-mail account from anywhere (TR. 25). E-mail accounts such as AOL reside on a server (TR. 25). A server is a computer system that holds information. (TR. 26). E-mail accounts physically store e-mail messages and attachments on servers (TR. 27). When an e-mail message is sent with an attachment, the person receiving the e-mail message would view the contents of the message and attachment from the server through their Internet browser (TR. 28). Accordingly, the images attached to the e-mails were located on the server as opposed to stored on the hard drive of Briles' computer (TR. 33).

LEGAL ANALYSIS

A. Improper Venue

Powers argues venue is improper in the District of Nebraska under [U.S. Const. art. III § 2](#), [U.S. Const. amend. VI](#), and [Fed. R. Crim. P. 18](#)., because Nebraska does not have a connection to the offense stated in the Indictment. Trials shall be held in the state where they were committed. **See** [U.S. Const. art. III § 2, cl. 3](#). Specifically, in all criminal prosecutions, the accused has a right to a trial in the state and district where the crime was committed. **See** [U.S. Const. amend. VI](#). Furthermore, the court must set the location of trial with regard to convenience of the defendant, any victim, and witness, and to the prompt administration of justice. **See** [Fed. R. Crim. P. 18](#). Powers argued he was never physically in Nebraska, and the computer he allegedly used was in Phoenix, Arizona (TR. 15). However, “any offense against the United States begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed.” [18 U.S.C. § 3237](#). Powers failed to demonstrate venue in the District of Nebraska would be improper. Although Powers may not have been physically present in Nebraska, and the computer used to facilitate the violation was located in Arizona,

venue would be proper in any district in which the offense began in one district, and was completed or committed in any other district. **See** [18 U.S.C. § 3237](#). Powers' violation of the Computer Fraud and Abuse Act (CFAA), [18 U.S.C. § 1030\(a\)\(2\)\(C\)](#), began in Arizona when he intentionally exceeded authorized access to Briles' e-mail account and sent e-mail messages containing compromising images of Briles. However, Powers' violation of [18 U.S.C. § 1030\(a\)\(2\)\(C\)](#) was completed in Nebraska. Briles resided in and was injured in Nebraska when Powers violated CFAA. Powers committed the violation in furtherance of tortious acts, specifically violations of Nebraska law under invasion of privacy and intentional infliction of emotional distress. Furthermore, e-mails were sent to recipients in Nebraska (TR. 38-39). Briles' coworker received an e-mail Powers sent, which contained all of the compromising images (Ex. 102, p. 1). The coworker subsequently forwarded the e-mail to Briles (Ex. 102, p. 2). Venue would not only be proper in the District of Arizona where the crime began, but also in the District of Nebraska where the crime was completed. Hence, Powers may be prosecuted in any district where such crime began, continued, or completed. Accordingly, the court finds venue is proper in the District of Nebraska.

B. Failure to State an Offense

Powers argues the Indictment failed to set forth sufficient facts and allegations to allege a violation of a crime, and the Indictment failed to state a plain, concise, and definite written statement of essential facts constituting an offense under [Fed. R. Crim. P. 7\(c\)\(1\)](#). Powers alleges the Indictment does not state a crime and the conduct, with respect to this case, is not what Congress contemplated when it enacted [18 U.S.C. § 1030\(a\)\(2\)\(C\)](#).

An indictment is constitutionally sufficient if it "contains the elements of the charged offense and fairly informs the defendant of the charge against him, and enables the defendant to plead an acquittal or conviction in bar of future prosecutions for the same offense." [United States v. Resendiz-Ponce](#), 549 U.S. 102, 108 (2007); **see also** [Hamling v. United States](#), 418 U.S. 87, 117 (1974). "An indictment is normally sufficient if its language tracks the statutory language." [United States v. Hayes](#), 574 F.3d 460, 472 (8th Cir. 2009) (citing [Hamling v. United States](#), 418 U.S. at 117). In this case, the Indictment satisfied the elements of a constitutionally sufficient indictment and concisely follows the statutory language of the CFAA, [18 U.S.C. § 1030\(a\)\(2\)\(C\)](#).

First, the Indictment mirrored the required elements of CFAA. The elements of the CFAA include: accessing the computer, either with or without authorization, and obtaining the information from a protected computer. **See** [18 U.S.C. § 1030\(a\)\(2\)\(C\)](#). Those elements are specifically stated in the Indictment and inform the defendant as to the charge against him. **See** [Filing No. 1](#). Second, the Indictment included specific elements to Powers' CFAA violation. The Indictment stated the CFAA violation was committed on or about March 3, 2009, until March 14, 2009, in furtherance of an invasion of privacy and intentional infliction of emotional distress, both tortious acts in violation of Nebraska state law. **See** [Filing No. 1](#). The dates of the violation gave adequate notice of when the alleged offense occurred and enabled Powers to respond to the charges without fear of future prosecutions for the same crime. **See** [Filing No. 1](#). In *Hamling*, the indictment was sufficient to allege the defendant mailed "obscene" material in violation of a particular statute. [418 U.S. at 117-18](#). Similarly in *Resendiz-Ponce*, the indictment pointed to a relevant a criminal statute and alleged the defendant, "on or about June 1, 2003, attempted to enter United States of America at or near San Luis in the District of Arizona." **See** [549 U.S. at 107-08](#). Accordingly, the court finds the Indictment set forth sufficient facts and allegations to allege a violation of a crime and the indictment stated a plain, concise, and definite written statement of essential facts constituting an offense under [18 U.S.C. § 1030\(a\)\(2\)\(C\)](#).

C. Void for Vagueness

Powers contends [18 U.S.C. § 1030\(a\)\(2\)\(C\)](#) fails void for vagueness because it does not provide sufficient warning of what conduct is prohibited and denied Powers due process of law as guaranteed by the Fifth Amendment to the United States Constitution. Under the Fifth Amendment, a statute must give a person of ordinary intelligence a reasonable opportunity to know what is prohibited. **See** [United States v. Washam, 312 F. 3d 926, 929, \(8th Cir. 2002\)](#). Powers alleges [18 U.S.C. § 1030\(a\)\(2\)\(C\)](#) was not enacted to protect personal computers. Instead, Powers argues, Congress intended the statute to protect financial and governmental institutions from intrusions by hackers seeking information or maliciously altering the computer systems (TR. 3).

Courts apply a two-part test to determine whether a statute is void for vagueness. **See** [United States v. Washam, 312 F. 3d at 929](#). The statute must provide adequate notice of

prohibited conduct and must not lend itself to arbitrary enforcement. **See id. at 929**. The CFAA is a valid statute and is not strictly applicable only to financial and governmental institutions. Under the CFAA, the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.” 18 U.S.C. § 1030(e)(6). In this case, Powers accessed the server that hosted Briles’ e-mail account with an authorized password. Powers exceeded the authorization for which the password was given, however, when he obtained compromising images of Briles from her e-mail messages, which were stored on the server, and ultimately sent e-mail messages containing those images. According to the language of the statute, the CFAA does not narrow the term “exceeds authorized access” to only include financial and government access. Furthermore, the CFAA sufficiently defines situations when an authorized user exceeds such access and does not lend itself to arbitrary enforcement.

A “protected computer” is defined as a computer:

- (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
- (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

18 U.S.C.A. § 1030(e)(2). While the term “protected computer” includes computers used in financial or government situations, the CFAA provides notice and extends coverage to computers used in or affecting interstate communication. Under the CFAA, the servers that hosted Briles’ e-mail account or contained the compromising images qualify as “protected computers” because the servers can be used in interstate communication. E-mail servers are able to send and receive e-mail messages from anywhere in the United States, which ability constitutes interstate communication. Accordingly, 18 U.S.C. § 1030(a)(2)(C) is not void for vagueness and provides sufficient notice and warning of prohibited conduct under the statute.

IT IS RECOMMENDED TO SENIOR JUDGE LYLE E. STROM that:

1. Powers' Motion to Dismiss for Improper Venue ([Filing No. 16](#)) be denied.
2. Powers' Motion to Dismiss the Indictment ([Filing No. 18](#)) be denied.

ADMONITION

Pursuant to [NECrimR 59.2](#) any objection to this Findings and Recommendations shall be filed with the Clerk of the Court within fourteen (14) days after being served with a copy of this Findings and Recommendations. Failure to timely object may constitute a waiver of any such objection. The brief in support of any objection shall be filed at the time of filing such objection. Failure to file a brief in support of any objection may be deemed an abandonment of the objection.

DATED this 4th day of March, 2010.

BY THE COURT:

s/Thomas D. Thalken
United States Magistrate Judge

*This opinion may contain hyperlinks to other documents or Web sites. The U.S. District Court for the District of Nebraska does not endorse, recommend, approve, or guarantee any third parties or the services or products they provide on their Web sites. Likewise, the court has no agreements with any of these third parties or their Web sites. The court accepts no responsibility for the availability or functionality of any hyperlink. Thus, the fact that a hyperlink ceases to work or directs the user to some other site does not affect the opinion of the court.